UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

35th Annual Nonprofit Organizations Institute

January 17-19, 2018
Austin, TX

Keeping an Eye on Privacy and Data Protection Risks

Wendell J. Bartnick

Author Contact Information:
Wendell J. Bartnick
Reed Smith LLP
Houston, TX

wbartnick@reedsmith.com
713.469.3838

INTRODUCTION

The rapidly growing number of data breaches in the news has introduced most Americans to the topic of "data privacy and protection." Almost each week, we learn that another large company has experienced one affecting millions of people. Big companies are not the only ones at risk. Smaller companies and non-profit organizations also have information and systems they do not want exposed to attackers or the public. In addition, security breaches are not the only way an organization's data can create legal and reputational risk. Privacy-related problems can also be the subject of negative publicity[1] and donor, beneficiary, and employee backlash. These privacy issues can be just as harmful to an organization as data security issues.

This paper will begin by describing the topics of privacy and data security at a high level and explaining the difference between them. It will also discuss the risks that can arise from not handling personal information appropriately or a failure to implement appropriate data security measures. Finally, this paper will dive deeper into one privacy topic and one data protection topic. With respect to data privacy, the paper will focus on website Terms of Use and privacy policies. With respect to data protection, it will focus on the characteristics of information security programs and on vendor management.

1. What are "Data Privacy" and "Data Protection"?

    a. *Privacy*

The concept of "privacy" relates to how organizations choose to collect, use, disclose, and dispose of personal information. Organizations should consider the privacy implications of collecting personal information from donors, beneficiaries or customers, and employees. How an organization uses and shares the personal information it collects, such as for marketing purposes, are also privacy considerations.

The scope of "personal information," protected by privacy laws, has broadened over time largely because there is no federal privacy statute. At the national level, the Federal Trade Commission ("FTC") regulates privacy and data protection under the Federal Trade Commission Act.[2] Under the law, the FTC has regulated privacy and data security by bringing enforcement actions against companies where their privacy and data security practices are allegedly deceptive or unfair.[3] The FTC has also issued guidance[4] it treats as a form of informal law, but it has not issued formal rules regulating privacy and data security.

---

[1] Natasha Singer, *InBloom Student Data Repository to Close*, NY TIMES BITS (Apr. 21, 2014), https://bits.blogs.nytimes.com/2014/04/21/inbloom-student-data-repository-to-close/.
[2] *See* Federal Trade Commission Act, 15 U.S.C. §§41-58.
[3] Fed. Trade Comm'n, LEGAL RESOURCES, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=247 [hereinafter FTC Legal Resources].
[4] *Id.*

The FTC had formerly created a dichotomy between personally identifiable information and non-personally identifiable information. Personally identifiable information includes information that can be readily used to identify or locate an individual, such as name, address, telephone number, email address, driver's license number, and social security number. However, the FTC has shifted away from using such distinction. In recent enforcement actions[5] and guidance[6] the FTC has broadened its view of information that should have privacy protections to include device identifiers and even television viewing information. Therefore, the regulatory trend in the United States is a broadening of the types of information that are "personal information."

While the U.S. does not have one federal privacy law, there are sector-specific privacy and data security laws that protect information in certain contexts, such as health, financial, background checks, telecommunications information, and children's data.[7] These laws also protect information that many would not consider personal information. For example, The Health Insurance Portability and Accountability Act ("HIPAA") regulates personal health information in certain circumstances, and such covered information may include device identifiers, IP addresses, and any other unique identifying number, characteristic, or code.[8] The Gramm-Leach-Bliley Act ("GLBA") regulates internet cookie information that financial institutions or their service providers collect from customers.[9] The Fair Credit Reporting Act requires that organizations provide notice and obtain consent from individuals before obtaining consumer reports, and imposes information disposal obligations on organizations that obtain them.[10] The Children's Online Privacy Protection Act ("COPPA") regulates persistent identifiers that can recognize users under the age of 13 over time and across different websites or online services, including customer numbers held in cookies, IP addresses, and device identifiers.[11] These laws are consistent with the trend that information that identifies devices, and not just individuals, may be considered personal information subject to privacy laws.

---

[5] Press Release, Fed. Trade Comm'n, VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions Without Users' Consent (Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.

[6] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, 22 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; Fed. Trade Comm'n, *Keeping Up With the Online Advertising Industry*, BUSINESS BLOG (Apr. 21, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry.

[7] E.g., Health Insurance Portability and Accountability Act Regulations, 45 C.F.R. §§ 160-164 (health); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6827 (financial); and the Children's Online Privacy Protection Act Regulations, 16 C.F.R. § 312 (children); Fair Credit Reporting Act 15 U.S.C. §§1681 et seq. (consumer reporting agencies); Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522, 2701-2711, 3121-3127 (electronic surveillance).

[8] *See* 45 C.F.R. § 164.514.

[9] *See* 16 C.F.R. § 313.3.

[10] *See* 15 U.S.C. § 1681.

[11] *See* 16 C.F.R. § 312.2.

Title search: Keeping an Eye on Privacy and Data Protection Risks

Also available as part of the eCourse
Answer Bar: New Boardmember Basics

First appeared as part of the conference materials for the
35th Annual Nonprofit Organizations Institute session
"Keeping an Eye on Privacy and Data Protection Risks"